UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,197	06/29/2001	Petrus Lambertus Adriaanus Roelse	NL000365	7563

24737 7590 11/23/2004

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,197	ROELSE, PETRUS LAMBERTUS ADRIAANUS	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/28/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 are presented for examination.

Specification

2. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(h) DETAILED DESCRIPTION OF THE INVENTION.
(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 3, 5, 6, and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 3, 5, 6, and 8 recite "p.sub.diff" and "p.sub.lin". Applicant did not define "p.sub.diff" and "p.sub.lin" distinctly in the claim or in the specification. Applicant is required to distinctly point out the claimed subject matter which applicant regards as the invention in response to this office action. (The correction is given in light of the submitted specification).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-2, 4, 6-7, and 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (Lee, Patent No.: US 6,314,186 B1) in view of Magliveras et al. (Magliveras, Patent Number: 6,038,317).

7. As per claim 1, Lee teaches a method for cryptographically converting an input data block into an output data block (Lee Col. 4 lines 39-51, and Fig. 1); the method including performing a non-linear operation on the input data block using an S-box based on a permutation (Lee Col. 4 lines 39-51, Fig. 1, and Col. 1 lines 59-65),

Lee does not explicitly teach selecting the permutation from a predetermined set of at least two permutations associated with the S-box,

However Magliveras teaches selecting the permutation from a predetermined set of at least two permutations associated with the S-box that reads on wherein the method includes each time before using the S-box (pseudo-)randomly selecting the permutation from a predetermined set of at least two permutations associated with the S-box (Magliveras Col. 6 lines 6-58),

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Magliveras with in the system of Lee because it would allow an efficient method of multiplying or factoring elements of the permutation groups (Magliveras Col. 1 lines 11-24). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to select the permutation from a predetermined set of at least two permutations associated with the s-box before using the s-box (pseudo-)randomly because it would make the system cryptographically stronger than a system in which each s-box consists of only one fixed permutation and fast execution.

As per claim 13, Lee teaches a system for cryptographically converting an input data block into an output data block; the method system including:

an input for receiving the input data block (Lee Fig. 1 No. 10);

a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation (Lee Col. 4 lines 39-51); and

an output for outputting the processed input data block (Lee Fig. 3 No. 60, and Col. 4 lines 39-51)

Lee does not explicitly teach a storage for storing a predetermined set of at least two permutations associated with an S-box;

selecting the permutation from a predetermined set of at least two permutations associated with the S-box,

However Magliveras teaches a storage for storing a predetermined set of at least two permutations associated with an S-box (Magliveras Col. 42 lines 30-65);

selecting the permutation from a predetermined set of at least two permutations associated with the S-box that reads on the processor being operative to, each time before using the S-box, (pseudo-)randomly selecting the permutation from the stored set of permutations associated with the S-box (Magliveras Col. 73 lines 1-44, and col. 6 lines 6-58),

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Magliveras with in the system of Lee because it would allow an efficient method of multiplying or factoring elements of the permutation groups (Magliveras Col. 1 lines 11-24). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to select the permutation from a predetermined set of at least two permutations associated with the s-box before using the s-box

(pseudo-)randomly because it would make the system cryptographically stronger than a system in which each s-box consists of only one fixed permutation and fast execution.

As per claim 2, Lee and Magliveras teach all the subject matter as described above. In addition Magliveras teaches a method, wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set (Magliveras Col. 1 lines 10-25, and col. 73 lines 17-44). The rational for combining are the same as claim 1 above.

As per claim 4, Lee and Magliveras teach all the subject matter as described above. In addition Lee teaches a method, wherein the differential characteristic has a probability equal to zero in at least one of the permutations (Lee Col. 2 lines 35-53).

As per claim 6, Lee and Magliveras teach all the subject matter as described above. In addition Lee teaches a method, wherein the data block consists of n data bits and each element of the set of permutations is a permutation on a set of 2.sup.n elements, represented by Z.sub.2.sup.n (Lee Col. 27 lines 65-col. 26 lines 14), where each non-trivial linear characteristic of each permutation in this set has a probability of at least 1/2-p.sub.lin and at most 1/2+p.sub.lin, the set of permutations being formed by permutations which have been selected such that for each non-trivial linear characteristic with probability of 1/2-p.sub.lin or 1/2+p.sub.lin in any of the permutations, this linear characteristic has a probability closer to 1/2 in at least one of the other

permutations of the set (Lee Col. 2 lines 35-53, and col. 5 lines 66-col. 6 lines 8).

As per claim 7, Lee and Magliveras teach all the subject matter as described above. In addition Lee teaches a method, wherein the linear characteristic has a probability equal to 1/2 in at least one of the permutations (Lee Col. 2 lines 35-53, and col. 5 lines 66-col. 6 lines 8).

As per claim 9, Lee and Magliveras teach all the subject matter as described above. In addition Magliveras teaches a method, wherein the set of permutations consists of two permutations (Magliveras Col. 73 lines 14-44). The rational for combining are the same as claim 1 above.

As per claim 10, Lee and Magliveras teach all the subject matter as described above. In addition Magliveras teaches a method, including performing the selection of the permutation under control of an encryption key (Magliveras Col. 12 lines 45-67). The rational for combining are the same as claim 1 above.

As per claim 11, Lee and Magliveras teach all the subject matter as described above. In addition Lee teaches a method, wherein the selection of the permutation is performed under control of one bit of the encryption key (Lee Col. 3 lines 22-34).

As per claim 12, Lee and Magliveras teach all the subject matter as described above. In addition Lee teaches a computer program product where the program product is operative to cause a

processor to perform the method of claim 1 (Lee Col. 5 lines 55-65).

8. Claims 3, 5, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. (Lee, Patent No.: US 6,314,186 B1) in view of Magliveras et al. (Magliveras, Patent Number: 6,038,317), and in further view of Applicant Admitted Prior Art (AAPA).

As per claim 3, Lee and Magliveras teach all the subject matter as described above. In addition Lee teaches a method, wherein the data block consists of n data bits and each element of the set of permutations is a permutation on a set of 2.sup.n elements, represented by Z.sub.2.sup.n (Lee Col. 27 lines 65-col. 28 lines 14),

Lee and Magliveras do not explicitly teach where each non-trivial differential characteristic of each permutation in this set has a probability of at p.sub.diff; the set of permutations being formed by permutations which have been selected such that for each non-trivial differential characteristic with probability of p.sub.diff in any of the permutations, this differential characteristic has a probability lower than p.sub.diff in at least one of the other permutations of the set.

However AAPA discloses where each non-trivial differential characteristic of each permutation in this set has a probability of at p.sub.diff; the set of permutations being formed by permutations which have been selected such that for each non-trivial differential characteristic with probability of p.sub.diff in any of the permutations, this differential characteristic has a probability lower than p.sub.diff in at least one of the other permutations of the set (AAPA Page 6 lines 26-page 7 lines 31).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of AAPA with in the system of Lee and Magliveras because it would allow to compensate a cryptographic weakness in one of the permutations by a corresponding strength in at least one of the other permutations of the set.

As per claim 5, Lee, Magliveras, and AAPA teach all the subject matter as described above. In addition AAPA discloses a method as claimed in claim 4, wherein n=4, and p.sub.diff=1/4 (AAPA Page 6 lines 26-32). The rational for combining are the same as claim 3 above.

9. As per claim 8, Lee, Magliveras, and AAPA teach all the subject matter as described above. In addition AAPA discloses a method, wherein n=4 and p.sub.lin=1/4 (AAPA Page 6 lines 26-page 27 lines 5). The rational for combining are the same as claim 3 above.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100